STRATEGY RESEARCH PROJECT

"WILL THE BLIND BE LEADING THE BLIND" THE CLIPPER CHIP CONTROVERSY AND ITS RELEVANCE TO INFORMATIONAL DOMINANCE OF THE BATTLEFIELD

BY

LIEUTENANT COLONEL WILLIAM P. MURRAY
TUFTS UNIVERSITY
SSC Fellow
United States Army

USAWC CLASS OF 1998

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

"Will the blind be leading the blind"
The Clipper Chip controversy and its relevance to informational dominance of the battlefield

Prepared by

LTC William P. Murray

US Army War College
USAR Senior Service College Fellow

Fletcher School of Law & Diplomacy

Disclaimer

Medford, Massachusetts
1998

ABSTRACT

During the 20th Century the bulk of cryptography research and use was controlled by the military. On April 16, 1993 the Clinton administration announced that the NSA had secretly developed a stronger algorithm to be integrated into a chip called "Clipper". The catch, however, was that the keys for the chip would remain in the hands of the U.S. government.

This paper will focus on U.S. assumptions that we can control the flow of these technologies. It will examine the debate around the Clipper chip and its "key escrow" requirements. By reviewing risk assessment, manageability and costs for this structure, one can readily view the scope and complexity of this particular government position.

The speed of technological change, driven by global market forces, is bypassing our abilities to control the development of encryption products. This change will challenge our basic concepts of informational dominance of the battlefield as envisioned in Department of Defense's Revolution in Military Affairs (RMA) paradigm.

Global demand for encryption devices is growing quickly. The United States is being faced with a choice; adapt to the market imperatives, which must include revising our RMA viewpoints, or be left behind and face the inevitable consequences both economically and militarily.

TABLE OF CONTENTS

Introduction

The earliest systems of encryption were the so-called "Caesar Ciphers" used by early generals to send secret messages. They used the simplest of algorithms. Another letter a certain distance away in the alphabet replaced each letter. For instance, 'A' would become 'E' and 'B' would become 'F'. Today the science of cryptology is an advanced form of mathematics filled with esoteric jargon like "graph isomorphism," "multiplexers," and "one-way hash functions".

During the 20th century, the bulk of cryptography has been controlled by the military. Since its inception, the National Security Agency (NSA) has done most of the U.S. research in encryption. By the 1970s, code-making and code-breaking became the vogue for U.S. mathematicians. Seeing this as a threat, the NSA wrested control from the National Science Foundation and started dictating which encryption algorithms were produced and how strong they could be.

Thus, when IBM produced its encryption chip (Lucifer) in 1974, the NSA exercised its influence to make it weaker than IBM had wanted. Instead of a 128-bit "key", Lucifer ended up with a 56-bit key, thereby reducing its strength by a factor of several million. Lucifer would evolve into the Data Encryption Standard (DES), an algorithm used by government and industry to encrypt its important data and to encode confidential telephone calls. By 1993, as computers became fast enough to potentially break DES's codes, the popularity of DES began to wane.

On April 16, 1993, the Clinton administration announced that the NSA had secretly developed a stronger algorithm. It was called Skipjack and relied on an 80-bit key, making it 16 million times stronger than DES. Skipjack's algorithm would be implemented via the Escrowed Encryption Standard and be called the Clipper chip. Clipper chips would be installed in telephones,

faxes, and modems. Eventually, similar chips by the name of Capstone could be installed in computers to encrypt files.

Cryptography

Cryptography is the conversion of data into a secret code for transmission over a public network. The original text, or plaintext, is converted into a coded equivalent called ciphertext via an encryption algorithm. The ciphertext is decoded (decrypted) at the receiving end and turned back into plaintext. The encryption algorithm uses a key, which is a binary number that is typically from 40 to 128 bits in length. The data is "locked" for sending by combining the bits in the key mathematically with the data bits. At the receiving end, the key is used to "unlock" the code, restoring it to its original binary form.

The difference between types of encryption is one of capability:

•40-bit encryption, also called international-grade encryption, means there are 240 possible keys that could fit into the lock that holds your account information. That means there are many billions (a 1 followed by 12 zeroes) of possible keys.

•128-bit encryption, also called domestic-grade encryption, means there are 288 (a three followed by 26 zeroes) times as many key combinations than there are for 40-bit encryption. That means a computer would require exponentially more processing power than for 40-bit encryption to find the correct key.

There are two cryptographic methods. The traditional method uses a secret key, such as the DES standard. Both sender and receiver use the same key to encrypt and decrypt. This is the fastest method, but transmitting the secret key to the recipient in the first place is not secure.

The second method is public-key cryptography, such as RSA, which uses both a private and a public key. Each recipient has a private key that is kept secret and a public key that is published

for everyone. The sender looks up the recipient's public key and uses it to encrypt the message. The recipient uses the private key to decrypt the message. Owners never have to transmit their private keys to anyone in order to have their messages decrypted; thus the private keys are not in transit and are not vulnerable.

Data Encryption Standard (DES)

DES is the National Institute of Science and Technology (NIST) standard secret key cryptography method that uses a 56-bit key. DES is based on an IBM algorithm, which was further, developed by the U.S. National Security Agency (NSA). It uses the block cipher method, which breaks the text into 64-bit blocks before encrypting them. DES decryption is very fast and widely used. The secret key may be kept a total secret and used over again. Or, a key can be randomly generated for each session, in which case the new key is transmitted to the recipient using a public key cryptography method such as RSA.

Rivest-Shamir-Adleman (RSA)

RSA is a highly secure cryptography method by RSA Data Security, Inc., Redwood City, CA. It uses a two-part key. The owner keeps the private key; the public key is published. The sender uses the recipient's public key and encrypts the data. It can then only be decrypted by the recipient's private key. However, RSA is very computation intensive and thus it is often used to create a digital envelope (RSA-encrypted DES key and DES-encrypted data). This method encrypts the secret DES key so that it can be transmitted over the network, but encrypts and decrypts the actual message using the much faster DES algorithm. RSA is also used for authentication by creating a digital signature. In this case, the sender's private key is used for encryption, and the sender's public key is used for decryption. As RSA chips get faster, RSA encoding and decoding lowers the cost and increases the computational power of the operation.

International Data Encryption Algorithm (IDEA)

A secret key cryptography method that uses a 128-bit key. Introduced in 1992, its European patent is held by Ascom-Tech AG, Solothurn, Switzerland. It uses the block cipher method, which breaks the text into 64-bit blocks before encrypting them.

Computational Costs

Modest increases in computational cost can produce vast increases in security. Encrypting information very securely (e.g., with 128-bit keys) typically requires little more computing than encrypting it weakly (e.g., with 40-bit keys). In many applications, the cryptography itself accounts for only a small fraction of the computing costs. One consequence of this uniformity of costs is that there is rarely any need to tailor the strength of cryptography to the sensitivity of the information being protected. Even if most of the information in a system has neither privacy implications nor monetary value, there is no practical or economic reason to design computer hardware or software to provide differing levels of encryption for different messages. It is simplest, most prudent, and thus fundamentally most economical, to employ a uniformly high level of encryption.

The design and implementation of the simplest encryption algorithms, protocols, and implementations is a complex and delicate process. Experience has shown that secure cryptographic systems are deceptively hard to design and build properly. Very small changes frequently introduce fatal security flaws. For example, since the system's introduction in 1993, several failures have been discovered in the U.S. Escrowed Encryption Standard, the system on which the Clipper Chip (key-recovery) is based. Non-key recovery systems, which have simpler requirements, can also be subject to exploitable flaws, often only discovered after the chip has been fielded.

In attempting to break a code, the kind of hardware used against an encryption algorithm depends on the scale of the cryptanalytic operation and the total funds available to the attacking enterprise. A Field Programmable Gate Arrays (FPGA) chip, costing approximately $400 mounted on a card, would on average recover a 40-bit key in five hours. A more determined commercial predator [1], prepared to spend $10,000 for a set-up with 25 ORCA chips [2], can find 40-bit keys in an average of 12 minutes. For $300,000 your solution would take an average of 24 seconds ($1,000,000 results in an average solution in 0.7 seconds, $3,000,000 an average of 0.18 seconds, $10,000,000 on average in 0.005 seconds).

It is the nature of brute-force attacks that they can be paralleled indefinitely. It is possible to use as many machines as are available, assigning each to work on a separate part of the problem. Hypothetically, twice as much computing power can be expected to find the right key in half the time.

A more efficient technological approach is to take advantage of commercially available FPGA. FPGA technology is fast and cheap. FPGAs function as programmable hardware and allow faster implementations of such tasks as encryption and decryption than conventional processors. FPGAs are widely available, and mounted on cards, can be installed in standard PCs just like sound cards, modems, or extra memory.

The Importance of Encryption

Electronically managed information touches almost every aspect of daily life in modern society. This rising tide of important, yet unsecured, electronic data leaves our society increasingly vulnerable to curious neighbors, industrial spies, rogue nations, organized crime, and terrorist organizations.

In the late 1980s and early 1990s, intruders usually exploited relatively simple weaknesses, such as poorly chosen passwords and misconfigured systems that allowed access to computer systems. But computer security officials have seen more sophisticated intrusions in recent years. They also have observed that skillful hackers are passing their knowledge to others who have less technical capability, sometimes through "do-it-yourself" software.

In one well-known incident in 1994, computer system administrators at an Air Force research lab in Rome, N.Y., learned that their network had been penetrated by an illegal wiretap program called a "sniffer" that had been secretly installed on one of the systems connected to the lab's network. An investigation found that two intruders had managed to gain complete access to all of the information on seven of the lab's computer systems and had gone undetected for five days. The intruders then used the systems as an Internet launching platform to delve into other military, government, commercial and academic sites around the world. The General Accounting Office later estimated that the incident cost the Defense Department more than $500,000 to investigate.

Paradoxically, although the technology for managing and communicating electronic information is improving at a remarkable rate, this progress generally comes at the expense of intrinsic security. In general, as information technology improves and becomes faster, cheaper, and easier to use, it becomes less possible to control (or even identify) where sensitive data flows, where documents originated, or who is at the other end of the telephone. More and more frequently cryptographic techniques will become the only viable approach to assuring the privacy and safety of sensitive information as these trends continues.

One of the most important of these areas concerns protection against systemic national vulnerabilities. Indeed, in areas in which confidence in and availability of a national information

network are most critical, nonconfidential uses of cryptography are even more important than are capabilities for confidentiality. For example, ensuring the integrity of data that circulates in the air traffic control system is almost certainly more important than ensuring its confidentiality. Likewise, ensuring the integrity (accuracy) of data in the banking system is often more important than ensuring its confidentiality. [3]

Encryption is a global product and industry. As of September 1997, corporations and individuals could select from 1,601 encryption products from over 941 firms in thirty countries. Of this total, 653 products are made outside the United States by 472 foreign firms. Foreign encryption makers continue to outrank U.S. producers in number, increase their product lines faster than do U.S. firms, and market encryption products that are just as strong as those produced in the United States. [4]

Law Enforcement

Law enforcement has been challenged by encryption technology, but not completely stymied by it. Other methods of law enforcement have been demonstrably effective in solving the majority of cases in which encryption blocked, either permanently or temporarily, the collection of some evidence. However, as encryption becomes more powerful and more available internationally, and as systems become more sophisticated and less vulnerable to attack, the collection of evidence from encrypted sources will pose increasing difficulties for law enforcement.

The 1968 Omnibus Crime Control and Safe Streets Act regulates wiretapping by law enforcement. Under this law wiretaps can only be used for certain serious crimes including bribery, murder, kidnapping, and narcotics trafficking and can only be used as a last resort. The law originally only covered oral communication, but the Electronic Communications Privacy Act

of 1986 extended the provisions to include computer data being transmitted over the wires as well. [5]

Key Recovery

Key recovery systems have gained currency due to the desire of government intelligence and law enforcement agencies to guarantee access to encrypted information without the knowledge or consent of encryption users. However, a properly designed cryptosystem makes it essentially impossible to recover encrypted data without knowledge of the correct key.

Key recovery encryption systems provide some form of access to plaintext outside of the normal channel of encryption and decryption. Key recovery is sometimes also called "key escrow." The term "escrow" became popular in connection with the U.S. government's Clipper Chip initiative, in which a master key to each encryption device was held "in escrow" for release to law enforcement.

Today the term "key recovery" is used as generic term for these systems, encompassing the various "key escrow," "trusted third-party," "exceptional access," "data recovery," and "key recovery" encryption systems introduced in recent years. Although there are differences between these systems, the distinctions are not critical for our purposes. All key-recovery systems require the existence of a highly sensitive and highly available secret key or collection of keys that must be maintained in a secure manner over an extended time period. These systems must make decryption of information quickly accessible to law enforcement agencies without notice to the key owners. These basic requirements make the problem of general key recovery difficult, expensive and potentially too insecure for many applications and users.

Key recovery is especially problematic in communications systems, such as encrypted cellular telephone calls, because it destroys the property of forward secrecy. A system with

forward secrecy is one in which compromising the keys for decrypting one communication does not reduce the security of other communications.

Forward secrecy is desirable and important for two reasons. First, it simplifies the design and analysis of secure systems, making it much easier to ensure that a design or implementation is in fact secure. Secondly, and more importantly, forward secrecy greatly increases the security and decreases the cost of such a system, since keys need to be maintained and protected only while communication is actually in progress.

Key recovery destroys the forward secrecy property, since the ability to recover traffic continues to exist long after the original communication has occurred. It requires that the relevant keys be stored instead of destroyed, so that later government requests for the plaintext can succeed. If the keys are stored, they can be compromised, but if destroyed, the threat of compromise ceases at that moment.

To prevent abuse, the keys would be "escrowed" to two government agencies, each possessing half of each Clipper key. When a law enforcement agency tapped a phone line that had been encrypted with the Clipper chip, it would present a warrant to the agencies that would provide the proper key, enabling decryption of the intercepted data or conversation. In February 1994 the Attorney General announced that these custodial agencies would be the National Institute of Standards and Technology and the Automated Systems Division of the Department of the Treasury. Both are agencies of the executive branch.

The ultimate goal of government-driven key recovery encryption, as stated in the U.S. Department of Commerce's recent encryption regulations, ``envisions a worldwide key management infrastructure with the use of key escrow and key recovery encryption items."[6]

The requirements put forward to meet law enforcement demands for such global key recovery systems include:

•Third-party/government accesses without notice to or consent of the user. Even so-called ``self-escrow'' systems, where companies might hold their own keys, are required to provide sufficient insulation between the recovery agents and the key owners to avoid revealing when decryption information has been released.

• Ubiquitous international adoption of key recovery. Key recovery helps law enforcement only if it is so widespread that it is used for the bulk of encrypted stored information and communications, whether or not there is end-user demand for a recovery feature.

•High-availability, around-the-clock access to plaintext under a variety of operational conditions. Law enforcement seeks the ability to obtain decryption keys quickly - within two hours under current U.S. and other proposed regulations. Few commercial encryption users need the ability to recover lost keys around the clock, or on such short notice. [7]

• Access to encrypted communications traffic as well as to encrypted stored data. To the extent that there is commercial demand for key recovery, it is limited to stored data rather than communications traffic.

However, it is difficult to exclude authentication and signature keys from a key recovery infrastructure of the kind proposed by the government, because some keys are used for both signature and encryption. Nor is it sufficient to exclude from the recovery system keys used only to protect financial transactions, since many electronic commerce schemes use keys that are general in scope. The same key might be used, for example, to encrypt personal electronic mail as well as to electronically sign contracts or authorize funds transfers. [8]

Current U.S. Government Policy

For many years, the United States has controlled the export of cryptographic technologies, products, and related technical information as munitions (on the U.S. Munitions List (USML) administered by the State Department). These controls have been used to deny potential adversaries access to U.S. encryption technology that might reveal important characteristics of U.S. information security products and/or be used to thwart U.S. attempts at collecting signals intelligence information. [9]

To date, these controls have been reasonably effective in containing the export of U.S. hardware-based products with encryption capabilities. However, software-based products with encryption capabilities and cryptographic algorithms present a more difficult challenge because they can more easily bypass controls and be transmitted across national borders.

At the same time, cryptography is inherently dual-use in character (more so than most other items on the USML), with important applications to both civilian and military purposes. This fact suggests to some that the export of all cryptography should be regulated under the Commerce Control List (CCL). However, the fact remains that cryptography is a particularly critical military application for which few technical alternatives are available.

Current U.S. Government policy generally limits exportable mass-market software that incorporates encryption for confidentiality to using the RC2 or RC4 algorithms with 40-bit keys. They allow exemptions only for software built with key-recovery mechanisms or for high-power, non-recoverable, encryption products designed for financial institutions. Anyone who receives a

license must assist in the development and implementation of a key-management infrastructure. [10]

The Clipper Chip

The clipper chip was developed by the National Security Agency (NSA) and programmed by Mykotronx, Inc. It is a cryptographic device intended to protect private communications. The clipper chip will be used to encrypt voice transmissions while a similar device known as Capstone is intended for use in the encryption of data. Each chip includes four components: 1) the skip jack encryption algorithm, 2) F, an 80-bit family key that is common to all chips, 3) N, a 30-bit serial number (this length may change), 4) U, an 80-bit secret key that unlocks all messages encrypted with the chip. The skip jack encryption algorithm is used to scramble the message. The F family key proceeds to decrypt the message at the other end of the line. The U key is held by the two government agencies.

The clipper chip came under fire because: 1) criminals wouldn't use phones equipped with the government chip; 2) foreign customers wouldn't buy communications gear for which the US held the keys; 3) the system for giving investigators access to the back door master codes was open to abuse; 4) no guarantee that some clever hacker wouldn't steal the keys.

Net Effects

The requirements of government key recovery are completely incompatible with those of commercial encryption users. The differences are especially acute in four areas: the kinds of data for which recovery is required, the kinds of keys for which recovery is required, the manner in which recoverable keys are managed, and the relationship between key certification and key

recovery. Government key recovery does not serve private and business users especially well. Similarly, the key management and key recoverability systems naturally arising in the commercial world do not adapt well to serve a government.

Any key recovery infrastructure, by its very nature, introduces a new and vulnerable path to the unauthorized recovery of data where one did not otherwise exist. This introduces at least two harmful effects. It removes the inherent guarantees of security available through non-recoverable systems, which do not have an alternate path to sensitive plaintext that is beyond the users' control. It also creates new concentrations of decryption information that are high-value targets for criminals or other attackers.

The nature of key recovery creates new high-value targets for attack of encryption systems. Key recovery agents need to maintain databases that hold the keys to the information and communications their customers most value. In many key recovery systems, the theft of a single private key (or small set of keys) held by a recovery agent that could unlock much or all of the data of a company or individual. Theft of a recovery agent's own private keys might provide access to an even broader array of communications, or might make it possible to easily spoof header information designed to ensure compliance with encryption export controls. The key recovery infrastructure will tend to create extremely valuable targets, more likely to be worth the cost and risk of attack.

Every encrypted communication or stored file will be required to include information about the location of its key retrieval information. This ``pointer" is a road map showing law enforcement how to recover the plaintext. It will also show unauthorized attackers where to focus their efforts.

The scale on which a government-access key recovery infrastructure must operate exacerbates many of the security problems with key recovery. The stated requirements of law enforcement demand the construction of highly complex key recovery systems. Demands on the speed and process for recovering keys will greatly increase the complexity of tasks facing those trusted with key recovery information. Any demands for ubiquitous worldwide adoption of key recovery will greatly increase the complexity and number of entities involved. Each of these will in turn have a significant impact on both the security and cost of any key recovery system.

The most immediately evident problem with key recovery may be the expense of securely operating the infrastructure required supporting it. In general, cryptography is an intrinsically inexpensive technology. There is little need for externally operated ``infrastructure" (outside of key certification in some applications) to establish communication or store data securely. Key recovery requires a complex and hence expensive and insecure infrastructure. The estimated key recovery system costs would be over $5 billion per year, in addition to the losses from current export controls.

Informational dominance of the battlefield

DOD's 1994 Annual Report holds that "the exploitation and control of space will enable U.S. forces to establish information dominance over an area of operations...the key to achieving success in future crises or conflicts." This success through exploitation and control is based on our abilities to "see" the adversary. However, by applying an empirical rule know popularly as "Moore's Law" (the computing power available for a given cost doubles every 18 months), this particular frame of reference becomes overly optimistic. Systems including encryption are not bounded by geographical constraints. Therefore, it is prudent to assume that these capabilities will be developed and eventually effect the outcome of these assumptions of dominance.

The rest of the world has come to appreciate the importance of space and information. With many nations striving to improve their capabilities in these media. Others have learned to piggyback on commercial, third party, or U.S. military capabilities. This may limit the U.S. ability to deny others access to such assets. So armed, others may be able to do considerable damage to U.S. interests, even if they cannot prevail in a conventional military sense. If the United States cannot ultimately prevent the diffusion and use of such assets, the U.S. military will have to learn to operate in a transparent environment that it could hitherto impose upon others, but could avoid for itself.

One such area of historic U.S. superiority is signals intelligence, our ability to extract information from an opponent's radioelectric signals. This superiority is based on the quantity, strength, and placement of U.S. listening devices, plus the computational power behind U.S. codebreaking efforts. Allied code-breaking skills may well have decided Midway and D-Day, the key battles of World War II's Pacific and Atlantic campaigns.

Historically, the contest between codemakers and codebreakers has alternately favored first one side then the other. In the last decade, this contest has broken in favor of codemakers. Signals, for example, are becoming harder to pick up thanks to digital technology, frequency-hopping and spread-spectrum technologies, plus the replacement of microwave with optical fiber for long-distance communications. The proliferations of encryption technology will not only exacerbate this particular problem but will also allow lagging adversaries to play "catch up".

National security authorities recognize quite clearly that future capabilities to undertake traditional signals intelligence will be severely challenged by the spread of encryption and the introduction of new communications media. In the absence of improved cryptanalytic methods, attempts at cooperative arrangements with foreign governments, and new ways of approaching the

information collection problem, losses in traditional signals intelligence capability would likely result in diminished effectiveness of the U.S. intelligence community. [11]

Summary & Conclusions

Cryptography is one important tool for protecting information that is very difficult for governments to control. Although cryptography cannot solve all problems, for those information security problems to which it is well suited, cryptography provides a number of capabilities that few other technologies can provide as effectively. Furthermore, the knowledge underlying good cryptography easily diffuses across national boundaries, and the United States does not have a monopoly on cryptographic technologies. The widespread nongovernment use of cryptography in the United States and abroad is inevitable in the long run.

Key recovery systems are inherently less secure, more costly, and more difficult to use than similar systems without a recovery feature. The massive deployment of key-recovery-based infrastructures to meet law enforcement's specifications will require significant sacrifices in security and convenience and substantially increased costs to all users of encryption. Furthermore, building the secure infrastructure of the breathtaking scale and complexity that would be required for such a scheme is beyond the experience and current competency of the field, and may well introduce ultimately unacceptable risks and costs.

Likewise, a domestic key-recovery system provides no compelling national security benefit if other countries do not implement similar systems abroad. Given the presence of foreign, unrecoverable encryption technology, domestic key-recovery systems will neither restrict determined criminal efforts nor grant law enforcement agencies substantially increased evidence-gathering capabilities against established criminal groups.

The problems of information vulnerability, the legitimacy of various national interests in individual privacy, international economic competitiveness, law enforcement, national security and world leadership all point to the need for a concerted effort to protect vital information assets of the United States in a world of ubiquitous computing and communications. Cryptography is an important element of a comprehensive approach to information security

The role of national cryptography policy should be to facilitate a judicious transition between today's world of high information vulnerability and a future world of greater information security. To help assure the continuing availability of strategic and tactical intelligence, efforts to develop alternatives to traditional signals intelligence collection techniques should be given high priority in the allocation of financial and personnel resources before products become widely used.

ENDNOTES

[1] institute survey of more than 500 companies, banks, universities and government agencies, 64 percent reported some type of breach during 1997, up from 48 percent in 1996. Although nearly three-quarters suffered financial losses from those breaches, less than half could quantify their losses.

[2]The cost of an AT&T ORCA chip that can test 30 million DES keys per second is $200. This is 1,000 times faster than a PC at about one-tenth the cost!

[3] Defense officials are convinced that any terrorist attack will be aimed mainly at commercial and industrial targets, rather than at military networks. That could complicate the federal government's response.

[4] The worldwide market for encryption products in 1996 was $2 billion. The U.S. market, representing slightly more than half the global market, topped $1 billion in 1996. Annual growth in this industry is projected to exceed 59 percent over the next five years, producing a worldwide industry that will be worth nearly $20 billion in the year 2002. Erik R. Olbeter and Christopher Hamilton, Finding the Key: Reconciling National and Economic Security Interests in Cryptography Policy, Economic Strategy Institute, April 1998

[5] The Department of Justice credits information gleaned through wiretaps as leading to more than 20,000 felony convictions since the early 1980s. This would not have been possible if the criminals had been using encryption systems the FBI could not break. Between 1978 and 1988 there were 7200 applications for electronic surveillance, only 11 were denied. There were 740 applications for wiretap surveillance in 1988. Of these, 738 were authorized, 676 were installed. Fifty-nine percent of wiretaps were authorized for narcotics investigations. Fourteen wiretaps were authorized for investigations of homicide and 1 was authorized for investigation of kidnapping. The remaining 288 wiretaps were authorized for investigation of other crimes, including gambling (126), bribery (32) theft (9), extortion (21), and racketeering (80). Twenty are documented as "other." These wiretaps resulted in 2486 arrests during 1988. In 1992, less than 900 wiretaps were issued to law enforcement agencies across the country. Administrative Office of the U.S. Courts. Report on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications Washington, D.C.: April, 1993.

[6] Dept. of Commerce, ``Interim Rule on Encryption Items," Federal Register, Vol. 61, p. 68572 (Dec. 30, 1996)

[7] For example, the recent British ``Trusted Third-Party" system proposes similar law enforcement demands, requiring one-hour turnaround time for TTP recovery agents. See U.K. Department of Trade and Industry, ``LICENSING OF TRUSTED THIRD-PARTIES FOR THE PROVISION OF ENCRYPTION SERVICES," (March 1997) (Public Consultation Paper).

[8] In fact, it is technically straightforward for two parties to use their authentication keys to negotiate encryption keys for secure communication. Any system that distributes trusted authentication keys would ipso facto serve as an infrastructure for private communication that is beyond the reach of government surveillance.

[9] The USML is designed to regulate technologies with such applications for reasons of national security; retention of some controls will mitigate the loss to U.S. national security interests in the short term, allow the United States to evaluate the impact of relaxation on national security interests before making further changes, and "buy time" for U.S. national security authorities to adjust to a new technical reality.

[10] "Such policies exert a substantial negative impact on U.S. economic security by denying export opportunities to U.S. telecommunications, software and computer companies and affording foreign companies an opportunity to get a foothold in the software security industry," the report said. Estimating lost sales and indirect effects, the report estimated a growing loss to the U.S. economy over the next five years totaling between $37 billion and $96 billion. In 1998, current policies would cost the economy from $1.4 billion to $6.8 billion rising to from $17.7 billion to $39 billion in 2002. , (ESI). * Erik R. Olbeter and Christopher Hamilton, Finding the Key: Reconciling National and Economic Security Interests in Cryptography Policy, Economic Strategy Institute, April 1998

[11] The Commission also heard concerns that the broader use of encryption technologies, especially software encryption, and the commercial pressure to limit or end export controls on encryption, constitute a serious threat to NSA's ability to produce quality signals intelligence in the future. Report of the commission on the Roles and Capabilities of the United States Intelligence Community, Preparing for the 21st Century, An appraisal of U.S. Intelligence, March 1, 1996

BIBLIOGRAPHY

Adams, James, The Next World War: How Computers Are Fighting the New World Wars. New York: Simon & Schuster Trade

Agre, Philip E., Editor, Technology & Privacy The New Landscape. Cambridge: M I T Press, Oct. 1997

Beckett, Brian, Introduction to Cryptolology & PC Security. New York: The McGraw-Hill Companies, Feb. 1997

BloomBecker, Jay J., Editor, Computer Crime, Computer Security, Computer Ethics. Santa Cruz: National Center for Computer Crime Data, Feb. 1986

Cohen, Fredrick B., Protection & Security on the Information Superhighway. New York: John Wiley & Sons, Incorporated, 1995

Cooper, J. Arlin, Computer & Communications Security Strategies for the 1990s. New York: The McGraw-Hill Companies, June 1989

Evans, Charles L. "U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets." North Carolina Journal of International Law & Commercial Regulation 19(Summer 1994): 469-490.

Finch, J. H., Editor, Computer Security; A Global Challenge. New York: Elsevier, Science, Aug. 1985

Ford, Warwick, Secure Electronic Commerce. Paramus: Prentice Hall, April 1997

Froomkin, A. Michael, "It came From Planet Clipper: the Battle Over Cryptographic Key 'Escrow'." The University of Chicago Legal Forum (1996): 15-75

Hoffman, Lance J., Editor, Building in Big Brother; The Cryptographic Policy Debate. New York: Springer-Verlag, New York, Incorporated, Nov. 1995

Jackson, Keith M., Secure Information Transfer - PC Encryption. Boca Raton: C R C Press, Incorporated, Dec. 1990

Kane, Pamela, PC Security & Virus Protection: The Ongoing War Against Information Sabotage. New York: Henry Holt & Company, Incorporated, June 1994

Kerben, Jason. "The Dilemma for Future Communication Technologies: How to Constitutionally Dress the Crypto-Genie." Journal of Communications Law & Policy 15 (Winter 1997): 125-152

King, Henry R. "Big Brother, the Holding Company: A Review of Key-Escrow Encryption Technology." Rutgers Computers & Technology Law Journal 21 (1995): 224-262

Kugler, Hans J., Editor, Computer Security The Practical Issues in a Troubled World, New York: Elsevier Science, Incorporated Feb. 1986

Kuttner, Robert. "How 'National Security' Hurts Competitivenesss." Harvard Business Review 69 (January-February 1991): 140-149.

Landreth, Bill, Out of the Inner Circle: The True Story of a Computer Intruder Capable of Cracking the Nation's Most Secure Computer Systems, Redmond: Microsoft Press, Feb. 1989

Markoff, John, Cyberpunk: Outlaws & Hackers on the Computer Frontier. New York: Simon & Schuster Trade, July 1992

Pipe, G. Russell, Editor, Assessing Data Privacy in the 1990's & Beyond. Washington: Center for Strategic & International Studies, March 1997

Regan, Priscilla M. Legislating Privacy Technology, Social Values, & Public Policy. Chapel Hill: University of North Carolina Press, Sept. 1995

Schneier, Bruce. The Electronic Privacy Papers Documents on the Battle for Privacy in the Age of Surveillance. New York: John Wiley & Sons, Incorporated, 1997

Security in Cyberspace, Challenges for Society: Proceedings of an International Conference. Santa Monica: The Rand Corporation, Nov. 1996

Slatalla, Michele. Masters of Deception: The Gang That Ruled Cyberspace. New York: HarperCollins Publishers, Incorporated, Jan. 1996

Steinbrecher, Bradley K. "The Impact of the Clinton Administration's Export Promotion Plan on U. S. Exports of Computers and High-Technology Equipment." University of Pennsylvania Journal of International Business Law 15 (Winter 1995): 675-703

Stephenson, Peter. Cyber Crime Investigation. Indianapolis: Macmillan Technical Publishing, Aug. 1997

United States. Committee to Study National Cryptographic Policy. Cryptography's Role in Securing the Information Society. 1996.

Van der Lubbe, Jan C. Basic Methods of Cryptography. New York: Cambridge University Press

Yung, Andrew W. "Regulating the Genie: Effective Wiretaps in dthe Information Age." Dickinson Law Review 101 (Fall 1996): 95-135.